

# Kaspersky Security for Windows Server のご紹介

ランサムウェアに対抗する「アンチクリプター」を搭載

株式会社カスペルスキー  
製品本部

# 目次

1. サーバーセキュリティがなぜ重要か？
2. Kaspersky Security for Windows Serverの概要
  - Kaspersky Security for Windows Serverの特長
  - 導入の効果
3. 機能紹介
  - ランサムウェアなどマルウェア感染の防止
  - パフォーマンスの最適化
  - 運用を容易にする管理機能
  - さまざまなIT環境に対応
  - システム要件



# サーバーセキュリティがなぜ重要か？

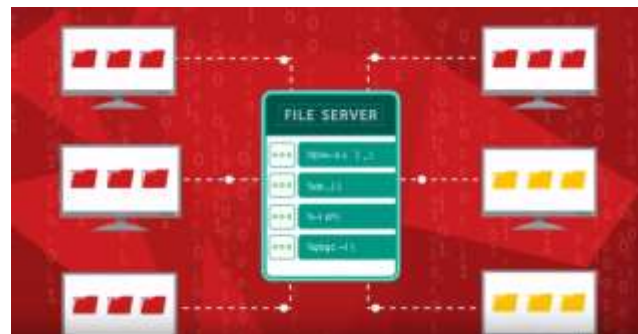
---

# サーバーセキュリティがなぜ重要か？

感染したマシンを經由して  
サーバーがマルウェアに感染すると…



サーバーに加え、サーバーを經由して  
各端末にも被害が拡大！



## PCの保護だけでなく、**サーバーの保護も重要**

- 重要な共有データの漏洩や、使用不可になることを防止
- サーバーを經由した感染の拡大を阻止



# Kaspersky Security for Windows Server の概要

---

# Kaspersky Security for Windows Server の特長

～複雑で高負荷なIT環境に対応し、ランサムウェアにも対抗～

## ▶ ランサムウェアより共有データを保護 (アンチクリプター)

- 共有フォルダ内のファイル1つでも悪意のある暗号化試行があった場合に、攻撃を仕掛けているコンピューターのアクセスをブロック

被害に遭うと  
データにアクセス不能...



## ▶ さまざまな構成に対応

- Server Coreモード、階層型ストレージ、ReFS (Resilient File System)、クラスター構成、ターミナルサーバーなど、法人利用におけるサーバーのさまざまな構成に対応

## ▶ 導入／アップデート時に再起動が不要

- インストールやアップデートの際に再起動が不要で、サーバーを停止する必要なし

# 導入の効果

～重要な業務データの漏洩や不正な暗号化による業務停止を阻止～



- ▶ ランサムウェアを含むマルウェアの脅威からサーバー上の重要データを強力に保護し、サーバーを経由した感染の拡大も阻止
- ▶ サーバーの用途に合わせてロードバランシングやスキャン設定を行うことで、サーバーへの負荷を調整してセキュリティを提供
- ▶ マルウェア検知などのイベントは管理者に通知され、対応を迅速に実施することが可能



# 機能紹介

---



# マルウェア感染の防止（1）

## ～多層防御の仕組みでマルウェアの脅威から保護～

### ▶ 既知だけでなく未知の脅威も検知

- ヒューリスティックアナライザ機能にて、エミュレーション環境でオブジェクトに悪意のあるコマンドシーケンスが含まれていないか検証し、疑わしい処理が検知された場合はブロック



### ▶ クラウドプロテクション（Kaspersky Security Network）

- カスペルスキーのクラウドに収集された世界中のリアルタイムの脅威情報をもとに、最新の脅威に迅速に対応し、誤検知も低減



### ▶ アプリケーション起動コントロール

- 不要なアプリケーションの起動をブロックすることでマルウェアへの感染リスクを低減
- アプリケーションの起動ルールを設定することで、実行ファイル、スクリプト、MSIパッケージの起動や、DLLモジュールのロードを許可／ブロック



# マルウェア感染の防止（２）

## ～ランサムウェアによる暗号化攻撃をブロック～

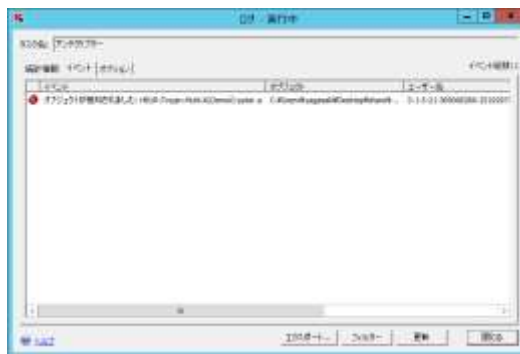
### ▶ アンチクリプター（悪意のある暗号化攻撃をブロック）

- 共有フォルダ内のファイル1つでも悪意のある暗号化試行があった場合に、攻撃を仕掛けているコンピューター（信頼しないホスト）のアクセスをブロック
- ブロックする時間は指定可能で、指定時間後はブロックが解除され、共有フォルダにアクセス可能
- 信頼しないホスト以外のPCからのアクセスはブロックしない

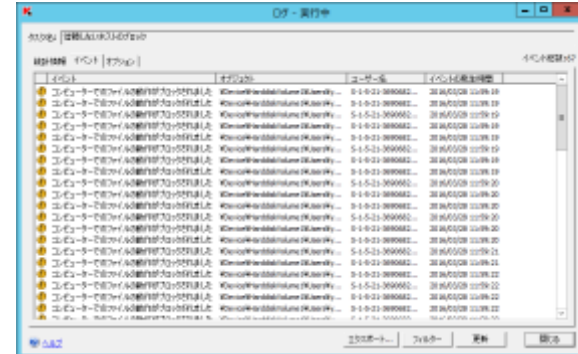
アンチクリプター管理者画面



検知時の画面



アクセスブロック時のログ画面



# パフォーマンスの最適化

## ～サーバー用途に合わせてセキュリティ強度とサーバー負荷を調整～

### ▶ ロードバランシング

- ・ 設定した優先度に応じて当アプリケーションと他のアプリケーション間でリソースを調整



### ▶ 柔軟なスキャン設定

- ・ スキャン強度の設定
- ・ アンチマルウェア処理のスレッド数を指定
- ・ スキャンの除外対象とするプロセスを指定（データのバックアップなど、信頼できるプロセス）
- ・ スキャンを実行する／しないファイル種別を指定
- ・ 疑わしい／感染したオブジェクトを検知した時の動作を設定

### ▶ スキャンの実行時間の設定

- ・ リアルタイムスキャンの他、オンデマンドでスキャンの開始／終了時間を指定可
- ・ 例えば、週末など、業務への影響が小さいタイミングを指定して、保護レベルを高めたフルスキャンの実施

# 運用を容易にする管理機能

～複数サーバーも一元管理し、イベント発生時は管理者に通知～



## ▶ 管理ツール

- ・ 統合管理サーバーKaspersky Security Center の他、Microsoft管理コンソール、コマンドラインを使用してサーバーセキュリティを管理

## ▶ インストールや運用の効率化

- ・ Kaspersky Security Centerにて複数サーバーへのリモートインストールや設定を同時に展開

## ▶ システム管理者への通知

- ・ 指定したイベントの発生時はEメールでシステム管理者に通知

# さまざまなIT環境に対応

～複雑で高負荷なWindowsサーバー環境も保護～

## ▶ クラスタ構成

- ローカルディスクおよびクラスタ構成で共有されているディスクを保護

## ▶ ターミナルサーバー

- WindowsリモートデスクトップサービスやCitrix社XenApp環境をサポート

## ▶ 仮想化環境

- VMware、Hyper-V、XenDesktopといった仮想化環境に対応



# システム要件

項目	サポート要件
ハードウェア	<p>【標準要件】</p> <ul style="list-style-type: none"><li>• CPU : x86 / x64互換のプロセッサ</li><li>• 空きディスク容量<ul style="list-style-type: none"><li>- アプリケーションインストール用 : 70 MB</li><li>- ウイルス定義データベース用 : 2 GB</li><li>- ログファイル用 : 1 GB</li><li>- 検疫、バックアップ保管用 : 400 MB</li></ul></li></ul> <p>【最小構成】</p> <ul style="list-style-type: none"><li>• CPU : 1.4 GHz、1コア</li><li>• メモリー : 1 GB</li><li>• ディスク : 4 GBの空き容量</li></ul> <p>【推奨構成】</p> <ul style="list-style-type: none"><li>• CPU : 2.4 GHz、4コア</li><li>• メモリー : 2 GB</li><li>• ディスク : 4 GBの空き容量</li></ul>
ソフトウェア	<p>【OS】 ※記載がない場合は64ビットOS</p> <ul style="list-style-type: none"><li>• Windows Server 2008 Standard / Enterprise / Datacenter SP1以降 (32/64ビット)</li><li>• Windows Server 2008 Core Standard / Enterprise / Datacenter SP1以降 (32/64ビット)</li><li>• Windows Server 2008 R2 Standard / Enterprise / Datacenter SP1以降</li><li>• Windows Server 2008 R2 Core Standard / Enterprise / Datacenter SP1以降</li><li>• Windows Server 2012 Essentials / Standard / Foundation / Datacenter</li><li>• Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter</li><li>• Windows Hyper-V Server 2008 R2 SP1以降</li><li>• Windows Hyper-V Server 2012</li><li>• Windows Hyper-V Server 2012 R2</li></ul> <p>【ターミナルサーバー】</p> <ul style="list-style-type: none"><li>• Windows Server 2008 リモート デスクトップ サービス</li><li>• Windows Server 2012 リモート デスクトップ サービス</li><li>• Windows Server 2012 R2 リモート デスクトップ サービス</li><li>• Citrix XenApp 6.0, 6.5, 7.0, 7.5, 7.6</li><li>• Citrix XenDesktop 7.0, 7.1, 7.5, 7.6</li></ul> <p>【その他】</p> <ul style="list-style-type: none"><li>• Microsoft Windows Installer 3.1</li></ul>

# THANK YOU

---

2016年4月版

Copyright © 2016 Kaspersky Lab. All rights reserved.

無断複写・転載を禁じます。カスペルスキー、Kaspersky®はKaspersky Labの商標または登録商標です。

**KASPERSKY**   
Save the World from IT threats